Chapter I

Lengendreovy a Jacobiho symboly

I.1 Legendreovy symboly

I.1.1 Definice. Nechť $p \in \mathbb{P}$ a $n \in \mathbb{Z}$. Legendreův symbol $\left(\frac{n}{p}\right)$ nabývá pouze tří hodnot, a sice 0, 1, -1. Tento symbol je definován takto:

(1) Jestliže $p \mid n$, pak $\left(\frac{n}{p}\right) = 0$;

(2) $\left(\frac{n}{2}\right) = 1$ pro každé n liché;

(3) Jestliže $p = 2k+1, k \in \mathbb{N}$, je liché prvočíslo a $p \nmid n$, pak $p \mid n^{2k}-1$, $n^{2k}-1 = (n^k-1)(n^k+1)$ (viz I) a nastává právě jeden z následujících případů:

   (a) $p \mid n^k - 1$ a $\left(\frac{n}{p}\right) = 1$;

   (b) $p \mid n^k + 1$ a $\left(\frac{n}{p}\right) - 1$.

I.1.2 Proposice. (Eulerovo kriterium). Nechť $n \in \mathbb{Z}$. Potom:

(i) $n \equiv \left(\frac{n}{2}\right) \ (mod\ 2)$.

(ii) Je-li $p = 2k+1 \in \mathbb{P}, k \in \mathbb{N}$, pak $n^k \equiv \left(\frac{n}{p}\right) \ (mod\ p)$.

Důkaz. Tvrzení plyne ihned z definice I.1.1. □

I.1.3 Lemma. Nechť $p \in \mathbb{P}$ a $n, m \in \mathbb{Z}$ jsou takové, že $n \equiv m \ (mod\ p)$. Potom $\left(\frac{n}{p}\right) = \left(\frac{m}{p}\right)$.

Důkaz. Tvrzení plyne snadno z I.1.1(1), I.1.1(2) v případě, že $p \mid n$ a $p = 2$. Ve zbylém případě stačí použít I.1.2(ii), neboť $n^k \equiv m^k \ (mod\ p)$ □

I.1.4 Lemma. $\left(\frac{nm}{p}\right) = \left(\frac{n}{p}\right)\left(\frac{m}{p}\right)$ pro všechna $n, m \in \mathbb{Z}$ a $p \in \mathbb{P}$.

Důkaz. Opět můžeme předpokládat, že $p \geq 3$, $p \nmid n$ a $p \nmid m$. Opět stačí použít I.1.2(ii), neboť $(mn)^k = n^k m^k$. □

I.1.5 Lemma. $\left(\frac{n^l}{p}\right) = \left(\frac{n}{p}\right)^l$ pro všechna $p \in \mathbb{P}$, $n \in \mathbb{Z}$ a $l \in \mathbb{N}$.

Důkaz. Tvrzení plyne snadnou indukcí z I.1.4. □

I.1.6 Proposice. Nechť $n \in \mathbb{N}$, $n \geq 2$ a nechť $n = p_1^{k_1} \dots p_m^{k_m}$ je prvočíselný rozklad čísla n (viz I). Pak $\left(\frac{n}{p}\right) = \left(\frac{p_1}{p}\right)^{k_1} \dots \left(\frac{p_m}{p}\right)^{k_m}$ pro každé prvočíslo p.

Důkaz. Stačí použít I.1.4 a I.1.5. □

I.1.7 Proposice. Nechť $p \in \mathbb{P}$ a $n \in \mathbb{Z}$. Potom:

(i) $\left(\frac{0}{p}\right) = 0$ a $\left(\frac{1}{p}\right) = 1$.

(ii) $\left(\frac{n}{2}\right) = \left(\frac{-n}{2}\right)$.

(iii) Je-li $p = 2k+1$ liché, $k \in N$, pak $\left(\frac{-1}{p}\right) = (-1)^k$ a $\left(\frac{-n}{p}\right) = \left(\frac{n}{p}\right)(-1)^k$.

Důkaz. (i) a (ii). Tvrzení plynou ihned z definice I.1.1.

(iii). Rovnost $\left(\frac{-1}{p}\right) = (-1)^k$ plyne ihned z I.1.2(ii) a zbylá rovnost plyne z I.1.4. □

I.1.8 Lemma. Nechť $p = 2k+1$ je liché prvočíslo. Potom nastává právě jeden z následujících dvou případů:

(1) $p \equiv 1, 7 \ (mod\ 8)$ a $2^k \equiv 1 \ (mod\ p)$;

(2) $p \equiv 3, 5 \ (mod\ 8)$ a $2^k \equiv 1 \ (mod\ p)$.

Důkaz. Případ $p = 3$ je zřejmý a budeme tedy předpokládat, že $p \geq 5$ (čili $k \geq 2$). Buď nyní r největší celé číslo takové, že $r \leq k$. Jistě je $1 \leq r \leq k$ a $2^k \cdot k! = (\prod_{i=1}^{r} 2i)(\prod_{i=r+1}^{k} 2i) \equiv (\prod_{i=1}^{r} 2i)(\prod_{i=r+1}^{k} (p-2i))(-1)^{k-r} \ (mod\ p)$, neboť $p - 2i \equiv (-1)2i \ (mod\ p)$. Nyní si uvědomíme, že $(\prod_{i=1}^{r} 2i)(\prod_{i=r+1}^{k} (p-2i)) = k!$.

Vskutku. Je-li j sudé číslo takové, že $2 \leq j \leq k$, pak $j = 2i$ pro nějaké i takové, že $1 \leq i \leq r$. Odtud plyne, že součin všech sudých čísel mezi 2 a k včetně je právě součin $\prod_{i=1}^{r} 2i$. Buď nyní j takové liché číslo, že $1 \leq j \leq k$. Číslo $p - j = 2k + 1 - j$ je sudé a $k + 1 \leq p - j \leq 2k$. Tedy $p - j = 2i$, kde $r + 1 \leq i \leq k$. Naopak, je-li $r + 1 \leq i \leq k$, pak $p - 2i$ je liché číslo a máme $1 \leq p - 2i \leq k - 1 + (k - 2r) \leq k$.

Všimneme-li si nyní, že $k-1+(k-2r)$ je právě nevětší liché číslo menší či rovné číslu k, vidíme též, že součin všech lichých čísel mezi 1 a k včetně je právě součin $\prod_{i=r+1}^{k}(p-2i)$.

Dokázali jsme rovnost $k! = (\prod_{i=1}^{r} 2i)(\prod_{i=r+1}^{k}(p-2i))$, z čehož plyne kongruence $2^k k! \equiv (-1)^{k-r}k!\ (mod\ p)$. Odtud $p \mid k!(2^k-(-1)^{k-r})$. Jelikož však je $k < p$ a $k! = 1\cdot 2\cdot 3\cdots k$, je též $p \nmid k!$, $p \mid (2^k-(-1)^{k-r})$ a $2^k \equiv (-1)^{k-r}\ (mod\ p)$.

Je-li $p = 8l+1$, pak $k = 4l$, $r = 2l$, $k-r = 2l$ a $2^k \equiv_p 1$. Je-li $p = 8l+7$, pak $k = 4l+3$, $r = 2l+1$, $k-r = 2l+2$ a $2^k \equiv_p 1$. Je-li $p = 8l+3$, pak $k = 4l+1$, $r = 2l$, $k-r = 2l+1$ a $2^k \equiv_p -1$. Nakonec je-li $p = 8l+5$, pak $k = 4l+2$, $r = 2l+1$, $k-r = 2l+1$ a opět $2^k \equiv_p -1$. Ovšem $-1 \equiv_p p-1$ a naše lemma je dokázáno. □

I.1.9 Věta. Nechť p je liché prvočíslo. Potom:

(i) $\left(\frac{2}{p}\right) = 1$ právě když $p \equiv 1, 7\ (mod\ 8)$.

(ii) $\left(\frac{2}{p}\right) = -1$ právě když $p \equiv 3, 5\ (mod\ 8)$.

Důkaz. Tvrzení plyne z I.1.2(ii) a I.1.8. □

I.1.10 Poznámka. Předchozí výsledky lze použít pro výpočet Legendreova symbolu $\left(\frac{n}{p}\right)$. Především podle I.1.7 se lze omezit na $n \geq 2$. Případ $p = 2$ je jasný z definice I.1.1 a lze se tedy omezit na liché prvočíslo p. Je-li n sudé číslo, $n = 2^r n_1$, $r = cont_2(n) \geq 1$, $n_1 \geq 1$ liché, pak $\left(\frac{n}{p}\right) = \left(\frac{2}{p}\right)^r \left(\frac{n_1}{p}\right)$ podle I.1.4 a I.1.5 a symbol $(\frac{2}{p})$ nalezneme pomocí I.1.9. Stačí tedy umět nalézt symbol $(\frac{n}{p})$ pro liché p a liché $n \geq 3$. Je-li $n = {p_1}^{k_1}\cdots {p_m}^{k_m}$ prvočíselný základ čísla n, pak p_i jsou vesměs lichá prvočísla a vzhledem k I.1.6 stačí znát symboly $\left(\frac{p_i}{p}\right)$.

Samozřejmě vzhledem k I.1.3 se lze omezit na $n < p$ (pak také $p_i < p$).

I.2 Věta o kvadratické reciprocitě

I.2.1 Věta. (Gaussovo kritérium). Nechť $p = 2k+1, k \in \mathbb{N}$, je liché prvočíslo a nechť $n \in \mathbb{N}$ je takové číslo, že $n \geq 2$ a $p \nmid n$. Budiž t počet těch čísel r takových, že $1 \leq r \leq k$ a $p \mid rn+s$ pro aspoň jedno s, $1 \leq s \leq k$. Potom $\left(\frac{n}{p}\right) = (-1)^t$ (čili $\left(\frac{n}{p}\right) = 1$ pro t sudé a $\left(\frac{n}{p}\right) = -1$ pro t liché).

Důkaz. Pro každé r takové, že $1 \leq r \leq k$, existuje jednoznačně určené číslo $c(r), 1 \leq c(r) < p$, tak, že $r_n \equiv c(r)\ (mod\ p)$. Je-li $c(r) \leq k$, položme $a(r) = 0$ a $b(r) = c(r)$. Je-li $k+1 \leq c(r)$, položme $a(r) = 1$ a $b(r) = p - c(r)$. V obou případech je $1 \leq b(r) \leq k$ a $rn \equiv (-1)^{a(r)}b(r)\ (mod\ p)$. Přímým výpočtem se přesvědčíme, že vzhledem k daným vlastnostem jsou čísla $a(r) \in \{0,1\}$ a $b(r) \in \{1,2,\ldots,k\}$ určena jednoznačně. Navíc je-li $b(r_1) = b(r_2)$ pro $1 \leq r_1 \leq r_2 \leq k$, pak je $r_2 n \equiv \pm r_1 n\ (mod\ p)$, čili budiž $p \mid (r_1 + r_2)n$ nebo $p \mid (r_2 - r_1)n$. Ovšem $p \nmid n$, čili buďto $p \mid r_1 + r_2$ a nebo $p \mid r_2 - r_1$. Ovšem $2 \leq r_1 + r_2 \leq 2k < p$, z čehož plyne $p \mid r_2 - r_1$. Je však $0 \leq r_2 - r_1 \leq k-1 < p$, a tak $r_2 = r_1$. Tím jsme dokázali, že b je prostá (nikoliv injektivní) transformace intervalu $\{1,2,\ldots,k\}$. Tento interval je konečná množina, b je její permutace a $1 \cdot 2 \cdots k = k! = b(1)b(2)\cdots b(k)$. Dále pak $k!n^k = 1n \cdot 2n \cdot 3n \cdots kn \equiv_p (-1)^{a(1)}b(1) \cdot p(-1)^{a(2)}b(2) \cdot p(-1)^{a(3)}b(3) \cdots p(-1)^{a(k)}b(k) = (-1)^a k!$, neboli $p \mid (n^k - (-1)^a)k!$, kde $a = \sum a(r)$. Jelikož $p \nmid k!$, vidíme, že $n^k \equiv (-1)^a\ (mod\ p)$, a tak $\left(\frac{n}{p}\right) \equiv (-1)^a$ plyne z I.1.2(ii). Vzhledem k tomu, že $\left(\frac{n}{p}\right), (-1)^a \in \{1,-1\}$, dostáváme přímou rovnost $\left(\frac{n}{p}\right) = (-1)^a$. Zbývá ověřit, že $a = t$. Nejprve si uvědomíme, že a je součet právě těch čísel $a(r)$, kde $a(r) = 1$. Je-li $1 \leq r \leq k$ takové, že $a(r) = 1$, pak $p \mid rn + b(r)$, kde $1 \leq b(r) \leq k$. Naopak jsou-li $1 \leq r \leq k$ a $1 \leq s \leq k$ taková, že $p \mid rn + s$, pak $rn \equiv -1 \cdot s\ (mod\ p)$, $a(r) = 1$ a $b(r) = s$. Tím je důkaz ukončen. □

I.2.2 Věta. (Věta o reciprocitě kvadratických zbytků). Nechť p, q jsou různá lichá prvočísla, $2k+1 = p \neq q = 2l+1, k, l \in \mathbb{N}$. Potom $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{kl}$.

Důkaz. Předpokládejme $q < p$, t.j. $l < k$. Označíme A množinu těch čísel r, že $1 \leq r \leq k$ a $p \mid rq + s$ pro nějaké s, $-l \leq s \leq k$. Pro $r \in A$ položíme $\alpha(r) = k + 1 - r$.

I.2.2.1 Lemma α je permutace množiny A a $\alpha^2 = id_A$ (tedy α je involuce na množině A).

Důkaz. Pro $r \in A$ je zřejmě $1 \leq \alpha(r) \leq k$. Dále $-p \mid rq + s, -l \leq s \leq k, -rq \equiv s\ (mod\ p), (k+1-r)q \equiv_p (k+1)q + s = (k+1)(2l+1) + s = 2kl + 2l + k + 1 + s = pl + k + l + 1 + s \equiv_p k + l + 1 + s \equiv l - k + s\ (mod\ p)$. Ovšem $-l \leq k - s - l \leq k$ a $p \mid ((k+1-r)q + k - l - s) = \alpha(r)q + k - l - s$. Tedy $\alpha(r) \in A$. Rovnost $\alpha^2 = id_A$ je zřejmá z definice transformace α. □

Položme $a = |A|$, t.j. a je počet prvků množiny A. Budeme dokazovat, že $(-1)^{kl} = (-1)^a$.

I.2.2.2 Lemma Je-li $1 \leq r \leq k$, pak $\alpha(r) = r$ právě když k je liché a $2r = k + 1$.

Důkaz. Ověříme snadným výpočtem. □

I.2.2.3 Lemma Nechť k je sudé. Pak $(-1)^{kl} = 1 = (-1)^a$.

Důkaz. Podle I.2.2.1 a I.2.2.2 je transformace α involuce definovaná na množině A a involuce α nemá pevný bod. Tedy množinu A lze rozložit na disjunktní sjednocení dvouprvkových podmnožin vzájemně permutovaných čísel. Odtud a je sudé a $(-1)^a = 1$. Ovšem kl je sudé též a $(-1)^{kl} = 1$.

I.2.2.4 Lemma Nechť k je liché a l sudé. Pak $(-1)^{kl} = 1 = (-1)^a$.

Důkaz. Číslo kl je sudé a $(-1)^{kl} = 1$. Stačí tedy dokázat, že involuce α nemá pevný bod (viz důkaz I.2.2.3). Číslo $k+1 = 2t$ je sudé, $t \in \mathbb{N}$. Vzhledem k I.2.2.2 je nutné a stačí dokázat, že $t \notin A$. Ovšem $2tq = (k+1)(2l+1) = 2kl + k + 2l + 1 = (2k+1)l + k + l + 1 = pl + 2v$, $2v = k + l + 1$ (číslo $k + l + 1$ je sudé). Tedy $p \mid 2(tq - v)$, $p \mid tq - v$ a $tq \equiv v \ (mod\ p)$. Zajisté $l < v \leq k$. Je-li nyní s takové, že $-l \leq s \leq k$, pak $1 \leq s + v \leq 2k < p$, a tak $p+s+v = (tq+s)-(tq-v)$. Jelikož $p \mid tq-v$, zjišťujeme, že $p \nmid tq+s$. Podle definice množiny A to znamená, že $t \notin A$, což jsme potřebovali dokázat. □

I.2.2.5 Lemma Nechť k i l jsou lichá čísla. Pak $(-1)^{kl} = -1 = (-1)^a$.

Důkaz. Máme $k+1 = 2t$ a $l+1 = 2v$, kde $t, v \in \mathbb{N}$. Opět $2tq = (k+1)(2l+1) = 2kl + 2l + k + 1 = (2k+1)l + k + l + 1 = p(l+1) - 2s$, $2s = k - l$ (číslo $k - l$ je sudé. Tedy $p \mid 2(tq+s)$ a $p \mid tq+s$. Zajisté $-l < 1 \leq s \leq k-2 < k$ a to znamená, že $t \in A$. Podle I.2.2.2 je t jediný pevný bod involuce α. Takž a je liché číslo a $(-1)^a = -1$. Součin kl je též lichý a $(-1)^{kl} = -1$. □

Dokázali jsme, že $(-1)^{kl} = (-1)^a$. K dokončení důkazu celé věty stačí (a je sudé) dokázat, že $(-1)^a = \left(\frac{p}{q}\right)\left(\frac{q}{p}\right)$. Pokračujme tedy.

Budiž B množina těch čísel r, že $1 \leq r_1 \leq k$ a $p \mid r_1 q + s_1$ pro aspoň jedno s_1 takové, že $1 \leq s_1 \leq k$. Je-li $b = |B|$, pak rovnost $\left(\frac{q}{p}\right) = (-1)^b$ plyne z I.2.1. Podobně je-li C množina těch čísel r_2, že $1 \leq r_2 \leq l$ a $q \mid r_2 p + s_2$ pro nějaké s_2, $1 \leq s_2 \leq l$, pak $\left(\frac{p}{q}\right) = (-1)^c$, kde $c = |C|$. Dohromady máme $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{b+c}$ a jak již víme, $(-1)^{kl} = (-1)^a$. Stačilo by tedy dokázat, že čísla a a $b+c$ mají stejnou paritu. My však dokážme více. Totiž ž $a = b + c$.

I.2.2.6 Lemma $B \subseteq A$

Důkaz. Inkluse plyne ihned z definic jednotlivých množin. □

I.2.2.7 Lemma $A = B \cup D$, kde $D = A \setminus B$. Přitom D je množina právě těch čísel r_3, že $1 \leq r_3 \leq k$ a $p \mid r_3q + s_3$ pro aspoň jedno s_3, $-l \leq s_3 \leq 0$ (potom $s_3 \leq -1$).

Důkaz. Opět stačí zvážit definice jednotlivých množin. □

Položíme-li $d = |D|$, pak máme $a = b+d$. K úspěšnému dokončení důkazu nám zbývá dokázat, že $c = d$. Za tím účelem nalezneme bijekci $\beta : C \to D$, tedy vzájemně jednoznačné zobrazení β množiny C na množinu D. Začneme následným přípravným lemmatem:

I.2.2.8 Lemma Nechť $r, t, s \in \mathbb{Z}$ jsou taková čísla, že $1 \leq r \leq l$, $1 \leq s \leq l$ a $rp = tq - s$. Potom $1 \leq t \leq k$.

Důkaz. Předně $tq = rp + s \geq p + 1$, z čehož ihned plyne $t \geq 1$. Buď nyní $v = t - k - 1$. Potom máme $tq = (k + 1 + v)(2l + 1) = 2kl + k + 2l + 1 + 2lv + v = (2k + 1)l + w = pl + w$, kde $w = k + 1 + l + v + 2lv$ a také $rp + s = tq = lp + w$ a $(l - r)p = s - w$. Jelikož $r \leq l$ a $s \leq l$, tak $s \geq w$ a $-k - 1 \geq s - l - k - 1 \geq v + 2lv = vq$. Odtud $t - k - 1 = v < 0$ a $t \leq k$. □

Buď $r \in C$. Podle definice množiny je $1 \leq r_2 \leq l$ a $r_2p = tq - s_2$, kde $t \in \mathbb{Z}$ a $1 \leq s_2 \leq l$. Snadno nahlédneme, že čísla t a s_2 jsou určena jednoznačně (plyne z nerovnosti $1 \leq s_2 \leq l$). Podle I.2.2.8 je $1 \leq \beta(r_2) = t$. Jelikož $-l \leq -s_2 \leq -1$, dostáváme $\beta(r_2) \in D$ (viz I.2.2.7). Tedy β je dobře definované zobrazení množiny C do množiny D.

I.2.2.9 Lemma Zobrazení β je injektivní (čili prosté).

Důkaz. Nechť $1 \leq r \leq r' \leq l$, přičemž $t = \beta(r) = \beta(r')$. Tedy $rp = tq - s$, $r'p = tq - s'$, kde $1 \leq s' \leq s \leq l$. Pak ovšem $p \mid (s - s')$, kde $0 \leq s - s' \leq l - 1 < p$. Odtud $s = s'$ a $r = r'$. □

I.2.2.10 Lemma Zobrazení β je na celou množinu D (čili surjektivní či projektivní).

Důkaz. Máme ověřit, že $\beta(C) = D$. Buď tedy $r_3 \in D$ (viz I.2.2.7). To jest $1 \leq r_3 \leq k$ a $p \mid r_3q + s_3$, $-l \leq s_3 \leq -1$. Máme $vp = r_3 + s_3$, $v \in \mathbb{Z}$ a jelikož $r_3q + s_3 \geq q - l = l + 1 \geq 2$, tak je $v \geq 1$. Rovněž $(l+1)p = (l+1)(2k+1) = 2lk+2k+l+1 > 2lk+2k = kq > r_3q+s_3 = vp$, z čehož plyne $v \leq l$. Celkově máme $1 \leq v \leq l$, $1 \leq -s_3 \leq l$ a $r_3q = vp+(-s_3)$. Podle definic množiny C a zobrazení β je $v \in C$ a $\beta(v) = r_3$. □

Z I.2.2.9 a I.2.2.10 plyne, že β je bijekcí množiny C na množinu D. Tedy $c = d$, $a = b + d = b + c$ a $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{b+c} = (-1)^{b+d} = (-1)^a = (-1)^{kl}$. Tím je důkaz celé věty nadobro skončen. □

I.3 Jacobiho symboly

I.3.1 Definice. Nechť $n, m \in \mathbb{Z}$, přičemž $m \geq 2$ a $m = p_1^{r_1} \cdots p_k^{r_k}$ je prvočíselný rozklad čísla m (kdy $r_i, k \in N$ a $p_1, \ldots, p_k$ jsou po dvou různá prvočísla). Tento rozklad je jednoznačný a my definujeme Jacobiho symbol předpisem

$$\left(\frac{n}{m}\right) = \left(\frac{n}{p_1}\right)^{r_1} \cdots \left(\frac{n}{p_k}\right)^{r_k},$$

kde $\left(\frac{n}{p_i}\right)$ jsou příslušné Legendreovy symboly (viz I.1.1). Opět $\left(\frac{n}{m}\right) \in \{0, 1, -1\}$. Položme ještě $\left(\frac{n}{1}\right) = 1$ pro $n \neq 0$ a $\left(\frac{0}{1}\right) = 0$. Tím jsme naši definici rozšířili i o číslo $m = 1$. Můžme psát $\left(\frac{n}{m}\right) = \prod_{p \in \mathbb{P}} \left(\frac{n}{p}\right)^{cont_p(m)}$ pro všechna $n \in \mathbb{Z}$ a $m \in \mathbb{N}$, kde buď to $n \neq 0$ nebo $m \neq 1$ (jako obvykle $0^0 = 1$).

I.3.2 Proposice. Nechť $n \in \mathbb{Z}$ a $m \in \mathbb{N}$ jsou taková čísla, že $NSD(n, m) \neq 1$ (t.j. čísla n a m jsou soudělná). Pak $\left(\frac{n}{m}\right) = 0$.

Důkaz. Je $m \geq 2$ a existuje $p \in \mathbb{P}$ tak, že $p \mid m$ a $p \mid n$. Pak $\left(\frac{n}{p}\right) = 0$ a rovnost $\left(\frac{n}{m}\right) = 0$ plyne ihned z definice tohoto symbolu (viz I.2.1).

I.3.3 Proposice. Nechť $n_1, n_2 \in \mathbb{Z}$ a $m \in \mathbb{N}$ jsou taková čísla, že $n_1 \equiv n_2 \ (mod\ m)$. Pak $\left(\frac{n_1}{m}\right) = \left(\frac{n_2}{m}\right)$.

Důkaz. Je-li $m = 1$, pak $n_1 = n_2$. Nechť $m \geq 2$ a nechť $p \mid m$, $p \in \mathbb{P}$. Jistě je $n_1 \equiv n_2 \ (mod\ p)$, a tudíž $\left(\frac{n_1}{p}\right) = \left(\frac{n_2}{p}\right)$ podle I.1.3. Zbytek je jasný z definice Jacobiho symbolů I.3.1. □

I.3.4 Proposice. Nechť $n_1, n_2 \in \mathbb{Z}$ a $m \in \mathbb{N}$. Pak $\left(\frac{n_1 n_2}{m}\right) = \left(\frac{n_1}{m}\right)\left(\frac{n_2}{m}\right)$

Důkaz. Opět lze předopkládat, že $m \geq 2$. Je-li $p \in \mathbb{P}$ takové, že $p \mid m$. pak $\left(\frac{n_1 n_2}{p}\right) = \left(\frac{n_1}{p}\right)\left(\frac{n_2}{p}\right)$ podle I.1.4. Zbytek je jasný. □

I.3.5 Proposice. Nechť $n \in \mathbb{Z}$ a $m_1, m_2 \in \mathbb{N}$. Pak $\left(\frac{n}{m_1 m_2}\right) = \left(\frac{n}{m_1}\right)\left(\frac{n}{m_2}\right)$.

Důkaz. Opět se lze omezit na čísla $m_1 \geq 2$ a $m_2 \geq 5$ (je $\left(\frac{0}{m}\right) = 0$ pro každé $m \in \mathbb{N}$). Je $cont_p(m_1 m_2) = cont_p(m_1) + cont_p(m_2)$ pro každé $p \in \mathbb{P}$ a zbytek je již jasný z definice Jacobiho symbolů. □

I.3.6 Proposice. Nechť $n_1, n_2 \in \mathbb{Z}$ a $m_1, m_2 \in \mathbb{N}$. Pak $\left(\frac{n_1 n_2}{m_1 m_2}\right) = \left(\frac{n_1}{m_1}\right)\left(\frac{n_2}{m_2}\right) \cdot \left(\frac{n_1}{m_2}\right)\left(\frac{n_2}{m_1}\right)$.

Důkaz. Tvrzení plyne snadnou kombinací I.3.4 a I.3.5. □

I.3.7 Proposice. Nechť $n, m \in \mathbb{N}$, $n \geq 2$, $m \geq 2$ a nechť $n = p_1^{r_1} \cdots p_k^{r_k}$ a $m = q_1^{s_1} \cdots q_l^{s_l}$ jsou příslušné prvočíselné rozklady. Potom je $\left(\frac{n}{m}\right) = \prod \left(\frac{p_i}{q_j}\right)^{r_i+s_j}$, $i = 1, \ldots, k, j = 1, \ldots l$.

Důkaz. Tvrzení plyne z I.3.4 a I.3.5. □

I.3.8 Proposice. Nechť $n \in \mathbb{Z}$ a $m \in \mathbb{N}$. Potom:
(i) $\left(\frac{0}{m}\right) = 0$ a $\left(\frac{1}{m}\right) = 1$.
(ii) Je-li $m = 2k + 1$ liché, $k \in \mathbb{N}_0$, pak $\left(\frac{-1}{m}\right) = (-1)^k$ a $\left(\frac{-n}{m}\right) = \left(\frac{n}{m}\right)(-1)^k$.

Důkaz. (i) Rovnosti plynou snadno z I.1.7(i) a definice I.3.1.

(ii) Je-li $m = 1$, pak $k = 0$ a $\left(\frac{-1}{1}\right) = 1 = (-1)^0$. Je-li m prvočíslo, pak rovnost $\left(\frac{-1}{m}\right) = (-1)^k$ je dokázána v I.1.7(iii). V obecném případě použijeme indukci prodle m. Je-li totiž $m \geq 9$ složné liché číslo, pak $m = m_1 m_2$, kde $m_i = 2k_i + 1$ jsou menší lichá čísla, $k_i \in \mathbb{N}$. Je $k = 2k_1k_2 + k_1 + k_2$ a $\left(\frac{-1}{m}\right) = \left(\frac{-1}{m_1}\right)\left(\frac{-1}{m_2}\right) = (-1)^{k_1} \cdot (-1)^{k_2} = (-1)^{k_1+k_2} = (-1)^k$ podle I.3.4. □

I.3.9 Proposice. Nechť $t \in \mathbb{N}$. Potom:
(i) $\left(\frac{-1}{2^t}\right) = 1$.
(ii) $\left(\frac{-n}{2^t}\right) = \left(\frac{n}{2^t}\right) = \left(\frac{n}{2}\right)^t$ pro každé $n \in \mathbb{Z}$.

Důkaz. (i) Je $\left(\frac{-1}{2^t}\right) = \left(\frac{-1}{2}\right)^t$ podle definice Jacobiho symbolu. Ovšem $\left(\frac{-1}{2}\right) = 1$ podle I.1.1(2).

(ii) Podle (i) a I.3.4 a I.3.5 je $\left(\frac{-n}{2^t}\right) = \left(\frac{-1}{2^t}\right)\left(\frac{n}{2^t}\right) = \left(\frac{n}{2^t}\right) = \left(\frac{n}{2}\right)^t$. □

I.3.10 Proposice. Nechť $m = 2^t m_1$, kde $t \in \mathbb{N}$ a $m_1 = 2k + 1$ je liché, $k_1 \geq 1$. Potom
(i) $\left(\frac{-1}{m}\right) = (-1)^{k_1}$.
(ii) $\left(\frac{-n}{m}\right) = \left(\frac{n}{m}\right)(-1)^{k_1}$ pro každé $n \in \mathbb{Z}$.

Důkaz. (i)Podle I.3.5 je $\left(\frac{-1}{m}\right) = \left(\frac{-1}{2^t}\right)\left(\frac{-1}{m_1}\right)$. Podle I.3.8 a I.3.7(i) dostáváme $\left(\frac{-1}{m}\right) = (-1)^{k_1}$.

(ii) Toto plyne z (i) s použitím I.3.4. □

I.3.11 Věta. Nechť $m \in \mathbb{N}$.
(i) Je-li m sudé, pak $\left(\frac{2}{m}\right) = 0$.
(ii) Je-li $m = 2k + 1$ liché, $k \in \mathbb{N}_0$, pak $\left(\frac{2}{m}\right) = (-1)^l$, kde $2l = k(k + 1)$ (či $8l = m^2 - 1$).

Důkaz. (i) Toto plyne ihned z I.3.2.

(ii) Je-li $m = 1$, pak $\left(\frac{2}{m}\right) = 1 = (-1)^0$, $l = 0$. Je-li $m \geq 3$ (liché) prvočíslo, pak rovnost $\left(\frac{2}{m}\right) = (-1)^l$ plyne snadno z I.1.9. Je-li m složné liché číslo, $m = m_1 m_2$, kde $m_1 \geq 3$ a $m_2 \geq 3$, pak budeme postupovat indukcí. Máme totiž $(m^2-1) - (m_1^2 - 1 + m_2^2 - 1) = m_1^2 m_2^2 - m_1^2 - m_2^2 + 1 = (m_1^2-1)(m_2^2-1) = (m_1-1)(m_1+1)(m_2-1)(m_2+1)$ a toto číslo je dělitelné číslem 16, čili $m^2 - 1 = 16t + m_1^2 - 1 + m_2^2 - 1 = 8(2t + l_1 + l_2) = 8l$, kde $8l_1 = m_1^2 - 1$, $8l_2 = m_2^2 - 1$ a $l = 2t + l_1 + l_2$. Podle indukčního předpokladu je $\left(\frac{2}{m_1}\right) = (-1)^{l_1}$ a $\left(\frac{2}{m_1}\right) = (-1)^{l_2}$. Podle I.3.5 je $\left(\frac{2}{m}\right) = \left(\frac{2}{m_1}\right)\left(\frac{2}{m_2}\right) = (-1)^{l_1+l_2} = (-1)^{l_1+l_2+2t} = (-1)^l$, $8l = m^2 - 1$. □

I.3.12 Věta. (Věta o reciprocitě pro Jacobiho symboly. Nechť $n = 2k+1$ a $m = 2l+1$ jsou dvě nesoudělná lichá čísla, $k, l \in \mathbb{N}_0$. Potom platí $\left(\frac{n}{m}\right)\left(\frac{m}{n}\right) = (-1)^{kl}$.

Důkaz. Rozdělíme jej do bodů.

(i) Je-li $n = 1$, pak $k = 0$ a $\left(\frac{1}{m}\right)\left(\frac{m}{1}\right)$. $1 = (-1)^0 = (-1)^{kl}$ podle I.3.7(i) a definice symbolu $\left(\frac{m}{1}\right)$ (viz I.3.1). Podobně je-li $m = 1$.

(ii) Jsou-li obě čísla již prvočísla, pak se použije věta I.2.2.

(iii) V obecném případě budeme postupovat indukcí podle $n + m$. Je-li m prvočíslo složné, pak $m = m_1 m_2$, kde $m_i = 2l_i + 1$, $l_i \in \mathbb{N}$ a máme $m = 2l+1$, $l = 2l_1 l_2 + l_1 + l_2$. Nyní $\left(\frac{n}{m}\right)\left(\frac{m}{n}\right) = \left(\frac{n}{m_1}\right)\left(\frac{m_1}{n}\right)\left(\frac{n}{m_2}\right)\left(\frac{m_2}{n}\right) = (-1)^{kl_1+kl_2} = (-1)^{k(l_1+l_2)+2kl_1l_2} = (-1)^{kl}$ podle I.3.4, I.3.5 a indukční předpokladu. Případ složného čísla n je symetrický. □

I.3.13 Poznámka. Pro úplnost bychom mohli definovat $\left(\frac{1}{0}\right) = 1$, $\left(\frac{-1}{0}\right) = -1$ a $\left(\frac{n}{0}\right) = 0$ pro $n \in \mathbb{Z}$, $n \neq 1, -1$. Nic důležitého by to však nepřineslo.

I.4 Trochu příkladů

K výpočtu Legendreových a Jacobiho symbolů slouží pravidla a rovnosti odvozené a získané v předchozích třech sekcích. Nejlépe bude si spočítat něco příkladů.

I.4.1 Příklad. Spočtěme Legendreův symbol $\left(\frac{6}{19}\right)$. Je $19 = 2 \cdot 9 + 1$ a my použijeme Gaussovo kriterium I.2.1. Máme $k = 9$, $1 \cdot 6 \equiv_{19} 6$, $2 \cdot 6 \equiv_{19} -7$, $3 \cdot 6 \equiv_{19} -1$, $4 \cdot 6 \equiv_{19} 5$, $5 \cdot 6 \equiv_{19} -8$, $6 \cdot 6 \equiv_{19} -2$, $7 \cdot 6 \equiv_{19} 4$, $8 \cdot 6 \equiv_{19} -9$ $9 \cdot 6 \equiv_{19} -3$. V I.2.1 označujeme číslo t počet záporných zbytků, což je v našem případě $t = 6$. Takže $\left(\frac{6}{19}\right) = (-1)^6 = 1$.

I.4.2 Příklad. Spočtěme $\left(\frac{11}{23}\right)$. Čísla $11 = 2 \cdot 5 + 1$ a $23 = 2 \cdot 11 + 1$ jsou lichá prvočísla a podle I.2.2 je $\left(\frac{11}{23}\right) = -\left(\frac{23}{11}\right)$. Dále $23 = 2 \cdot 11 + 1$, čili $\left(\frac{23}{11}\right) = \left(\frac{1}{11}\right) = 1$ podle I.1.3 a I.1.7(i). Celkově je $\left(\frac{11}{23}\right) = -1$.

I.4.3 Příklad. Spočtěme $\left(\frac{13}{37}\right)$. Je $13 = 2 \cdot 6 + 1$, $37 = 2 \cdot 18 + 1$ a $\left(\frac{13}{37}\right) = \left(\frac{37}{13}\right)$ podle I.2.2. Dále, $37 = 2 \cdot 13 + 11$, $\left(\frac{37}{13}\right) = \left(\frac{11}{13}\right) = \left(\frac{13}{11}\right) = \left(\frac{2}{11}\right) = -1$ (použij I.1.3, I.2.2, I.3.12 a I.1.9 (ii)). Tedy $\left(\frac{13}{37}\right) = -1$.

I.4.4 Příklad. Spočtěme $\left(\frac{19}{257}\right)$. Opět $19 = 2 \cdot 9 + 1$ a $257 = 2 \cdot 128 + 1$ jsou lichá prvočísla. Je $\left(\frac{19}{257}\right) = \left(\frac{257}{19}\right)$ podle I.2.2. Dále, $257 = 13 \cdot 19 + 10$, a tak $\left(\frac{257}{19}\right) = \left(\frac{10}{19}\right) = \left(\frac{2}{19}\right) \cdot \left(\frac{5}{19}\right) = -\left(\frac{5}{19}\right)$ podle I.1.3, I.1.4 a I.1.9(ii). Ovšem $\left(\frac{5}{19}\right) = -\left(\frac{19}{5}\right) = -\left(\frac{4}{5}\right) = -\left(\frac{2}{5}\right)^2 = -1$ (opět se použije I.2.2, I.1.3 a I.1.4. Tedy $\left(\frac{19}{257}\right) = -1$.

I.4.5 Příklad. Spočtěme Jacobiho symbol $\left(\frac{506}{3309}\right)$ ($2 \mid 506$ a $3 \mid 3309$). Nejdříve pomocí XXX zjistíme, že čísla 506 a 3309 jsou nesoudělná. Dále, $506 = 2 * 253$ a tak $\left(\frac{506}{3309}\right) = \left(\frac{2}{3309}\right) \cdot \left(\frac{253}{3309}\right)$. Podle I.3.10 je $\left(\frac{2}{3309}\right) = (-1)^l$, kde $2lje1654 \cdot 1655$, čili $l = 827 \cdot 1655$ (je totiž $3309 = 2 \cdot 1654 + 1$). Tedy $\left(\frac{2}{3309}\right) = -1$, neb l je liché, a máme $\left(\frac{506}{3309}\right) = -\left(\frac{253}{3309}\right)$. Nyní, $\left(\frac{253}{3309}\right) = \left(\frac{3309}{253}\right)$ podle I.3.11 (neb $k = 1654$ je sudé), $3309 = 13 \cdot 253 + 20$, $\left(\frac{3309}{253}\right) = \left(\frac{20}{253}\right) = \left(\frac{2}{253}\right)^2 \cdot \left(\frac{5}{253}\right) = \left(\frac{5}{253}\right)$ podle I.3.3 a I.3.4. Avšak, podle I.3.11, je $\left(\frac{5}{253}\right) = \left(\frac{253}{5}\right) = \left(\frac{3}{5}\right) = \left(\frac{5}{3}\right) = \left(\frac{2}{3}\right) = -1$ (opět se použije I.3.3 a I.3.11. Dohromady dostáváme $\left(\frac{506}{3309}\right) = 1$.

I.4.6 Příklad. Spočtěme $\left(\frac{713}{3511}\right)$. Jde vlastně o Legendreův symbol, neboť 3511 je prvočíslo. Ale to nebudeme potřebovat. Je také $713 = 23 \cdot 31$, ale ani to nepotřebujeme vědět. Předně, $3511 = 2 \cdot 1755 + 1$ a $713 = 2\ cdot356 + 1$. Dále se přesvědčíme, že čísla 713 a 3511 jsou nesoudělná. Podle I.3.11 je $\left(\frac{713}{3511}\right) = \left(\frac{3511}{713}\right)$. Jelikož $3511 = 5 \cdot 713 + 669$, tak je $\left(\frac{3511}{713}\right) = \left(\frac{669}{713}\right)$. Čísla 669 a 713 jsou nesoudělná a $\left(\frac{669}{713}\right) = \left(\frac{713}{669}\right)$ podle I.3.11. Nyní, $713 = 669 + 44$, $\left(\frac{713}{669}\right) = \left(\frac{44}{669}\right) = \left(\frac{2}{669}\right)^2 \cdot \left(\frac{11}{669}\right) = \left(\frac{669}{11}\right) = \left(\frac{9}{11}\right) = \left(\frac{3}{11}\right)^2 = 1$. Celkově $\left(\frac{713}{3511}\right) = 1$.

I.4.7 Poznámka. Jacobiho symboly zobecňují symboly Legandreovy a početní pravidla pro jejich výpočty jsou obdobná. Nicméně si všimněme, že při výpočtu Jacobiho symbolů (keré ovšem zahrnují i Legandreovy symboly) nepotřebujeme rozkládat daná čísla na součin prvočísel, což bývá v případě velkých čísel obtížné (srovnej s I.1.10).

Při výpočtech použijeme především I.3.3, I.3.4, I.3.5, I.3.9, I.3.3, I.3.10 a I.3.11.